

SYSTEM AND METHODS FOR FLEXIBLE, CONTROLLED
ACCESS TO SECURE REPOSITORY SERVER STORED
INFORMATION

Inventors:

Jackie Zhanhong Wu
William W. Rose
Steven T. Kirsch
Satish Natarajan
Russell D. Wyllie
Charles Kline

1
2 SYSTEM AND METHODS FOR FLEXIBLE, CONTROLLED
3 ACCESS TO SECURE REPOSITORY SERVER STORED
4 INFORMATION
5

6 Inventors:

7 Jackie Zhanhong Wu
8 William W. Rose
9 Steven T. Kirsch
10 Satish Natarajan
11 Russell D. Wyllie
12 Charles Kline
13

14 Cross-Reference to Related Applications

15 The present application is related to the following Applications, assigned
16 to the Assignee of the present Application, which are incorporated herein by
17 reference:

18 1) System and Methods for Integration of a Web Site with a Repository
19 Server, Wu et al., Serial No. _____, filed concurrently herewith;

20 2) Secure User-Information Repository Server Accessible Through A
21 Communications Network, Wu et al., Serial No. _____, filed concurrently
22 herewith; and

23 3) Automatable Secure Submission of Confidential User Information Over
24 a Computer Network, Wu et al., Serial No. _____, filed concurrently
25 herewith.
26

Background of the Invention

Field of the Invention:

The present invention is generally related to public network connected data repository systems used to store user-information and, in particular, to a network-accessible secure repository server system that stores confidential user-information for access by third-parties subject to user and system defined constraints and conditions.

Description of the Related Art:

The use of the Internet and other public and private networks to transfer confidential user information continues to grow. In particular, business-to-consumer and business-to-business electronic commerce (e-commerce) sites require secure electronic transactions involving confidential user information to complete purchases. Other sites rely on confidential user information to tailor their site appearance and store prior activities for the benefit of individual users. While some information may be stored on the user computer systems in the form of cookies, the typical requirement is for the user to explicitly establish a site account, with a unique site-identity, to store confidential user-information persistently with the site.

With each new site-account established, the user is burdened with the requirement of maintaining a record of the account, managing the stored user information, and handling the status and confirmations of transactions conducted through each account. This typically requires the user to independently remember a unique user name and password for each account, manually update each and every active merchant account with any changes in billing address, shipping

1 address and credit card information, and to individually manage the processes
2 of confirming electronic transactions, receiving transaction receipts, and
3 monitoring the status of transactions not yet delivered.

4 While the overall burden of managing an individual site-account may not
5 be large, a typical user will often have a relatively large number of such accounts.
6 As a result, the total burden of fully maintaining more than a few accounts
7 becomes rather impractical. Even for businesses needing to maintain accounts
8 with multiple merchant vendors, the individuality of the site-account presentations,
9 modification methods, and information requirements represents a substantial
10 burden.

11 The nature and effects of this burden have been recognized for some time.
12 A number of potential solutions have been implemented in various manners,
13 though with only marginal success. These solutions are generally categorized as
14 electronic wallets, or data repositories, where the confidential user data is stored
15 locally on the user's own computer system or on a remote, network connected,
16 centralized repository server. Conventional e-wallets, however, have failed to
17 become more than marginally accepted or used for a variety of fundamental
18 reasons.

19 For example, local e-wallet applications, such as Gator™ (www.gator.com),
20 provides somewhat limited security for user information stored on the user
21 computer system. In operation, the application intercepts URL requests to selected
22 Web pages, typically the order checkout-form pages, of e-commerce sites
23 previously recorded in the application's local repository, which also records the
24 form layout and data requirements of each page. Some layout and requirements
25 analysis may be performed by the application to account for discrepancies and

1 changes in the Web pages with the result that recognizable form fields are filled-in
2 by the application based on the user information stored in the local repository.
3 This analysis capability is typically extended to attempt to identify Web-form pages
4 and then recognize the specific data requirements of these pages.

5 The ability of e-wallet applications to reliably discern the specific data
6 requirements of different fields on unknown Web-page forms from multiple
7 unknown sites, and even known sites with changed Web-page forms, is lacking.
8 A significant degree of user intervention is required to compensate for
9 unpredictable form identification and data requirement errors. Furthermore, the
10 matching and processing of available user data to the specific data requirements
11 of a Web-page form is also often unreliable, resulting in the potential for user
12 information to be improperly submitted.

13 Thus, conventional local e-wallet applications have failed to gain
14 acceptance due to a variety of reasons, including limited ability for the user to
15 differentially control access to the user's information, inadequate security
16 protections, inability to access the e-wallet information globally, and too frequent
17 unreliable identification the data requirements and fill-in of particular fields in ever
18 changing Web-page forms.

19 Conventional remotely located repository applications, such as Microsoft®
20 *Passport* (www.passport.com), use a network server as a central repository for
21 confidential user information. Other, typically e-commerce servers are required
22 to tightly integrate with the *Passport* server in order to securely and reliably request
23 and receive confidential user information. The Web-page form owner is therefore
24 required to maintain all form fields in strict conformance with the requirements of
25 the *Passport* system in order to receive information from the remote repository

1 server. There is also little or no flexibility for the definition and use of form-fields
2 uniquely required, let alone desired, by a particular participating site.
3 Consequently, any participating site must adopt a specific and proprietary coding
4 nomenclature for binding the *Passport* system to their Web-page form fields.
5 These integration requirements are recognized to be beyond the practical
6 capabilities of non-commercial sites. Further, the inability to define and use
7 unique fields greatly restricts the *Passport* system from being used by sites with
8 non-generic user data requirements.

9 The burdensome design, implementation, and management requirements
10 imposed on each participating site, as well as the enforced inflexibility for
11 handling new and unique types of information represents a substantial barrier to
12 more than marginal acceptance of such remote repository systems. While
13 conventional *Passport*-type systems generally provide much stronger security over
14 confidential user data and, by definition, reliability to fill-in forms, they provide
15 little or insufficient user capabilities to manage user data and differentially control
16 access to that information by participating sites. For these reasons, the *Passport*
17 system has met with very limited adoption.

18 A public standard, known as the Electronic Commerce Modeling Language
19 or ECML (www.ecml.org), has been proposed and met with some limited
20 acceptance. This standard, in effect, merely defines a limited set of names for
21 form fields used by merchants to define a credit-card e-commerce transaction.
22 The defined fields allow specification of a shipping address, billing address,
23 receipt address, the essential details of single credit card, and a very small set of
24 order management fields including little more than an order ID field and a
25 transaction complete field. Thus, the field definitions are sufficient for an e-

1 commerce merchant to submit a credit card number for validation with the card
2 issuer's databases. The ECML standard does not, however, provide for any actual
3 implementation. Rather, the ECML field definitions allow e-commerce system
4 vendors to implement their own credit-card validation services with only a
5 potential for interoperability based on the form naming convention. Further, no
6 provision is made for supporting the validation or storage and retrieval of any
7 additional, let alone non-credit-card, information.

8 Consequently, none of the known repository-based systems are capable
9 of meeting the broad needs of users to store and define access to their user
10 information in a manner that is secure, flexible enough for use among many
11 participating sites, and sufficiently easy to adopt and maintain by both users and
12 the many different types of potential participating sites.

13 14 Summary of the Invention

15 Thus, a general purpose of the present invention is to provide for the
16 secure storage of flexibly-defined confidential user information from a remote
17 repository server and selective provision of the information to any site partnered
18 with the remote repository server system subject to flexibly-defined constraints and
19 conditions.

20 This is achieved in the present invention by establishing a repository server
21 system to store confidential user-information for selective distribution, on behalf
22 of a user to third-party server systems to enable autonomous form data fill-in of
23 named form fields having third-party server defined data formats. A database is
24 utilized to store the confidential user-information data in named data fields. A
25 repository server processor is coupleable to the database to obtain access to the

1 confidential user-information. The processor is also coupleable to a
2 communications network to receive a form data request issued by the third-party
3 server. The form data request includes a predefined selective mapping of named
4 form fields relative to the named data fields. The processor operates over the
5 selective mapping to access the confidential user-information data and produce
6 instances of the confidential user-information data corresponding to the defined
7 data formats of the named form fields. A form data response, then returned to
8 the third-party server system, contains the confidential user-information data
9 corresponding to the defined data formats of the named form fields.

10 Selective delivery of confidential user-information is also achieved in the
11 present invention by providing a user identification system that establishes secure
12 and selectively controlled release of information associated with a user
13 identification. The repository server system supports secure network
14 communications with a user and with third-party sites remote from the repository
15 server system. The user and third-party sites pre-establish user and third-party
16 accounts with the repository server system, each receiving an identifying reference
17 recognizable by the server system. The request for information received by the
18 repository server system includes the third-party identity reference and is
19 accompanied by the client identity reference. User account data access in
20 response to the received request is first qualified by data access rules established
21 by the user. Depending on these user established data access rules, the repository
22 server system selectively initiates a communications session with the user, in effect,
23 while the received request is pending with the repository server system, to obtain
24 user responses to the request for and approve release of the user-information to
25 the third-party site.

1 An advantage of the present invention is that a flexible profiling system
2 allows the user to define and control any and all particular confidential user-
3 information that can be accessed, altered, and provided to individual partner
4 sites. The partner sites may be further constrained by a repository enforced typing
5 of any partner to further protect against the inappropriate accessing, altering, or
6 provision of confidential user-information to partner sites. Additionally, a system
7 of sub-profiles or related profiles to be established to allow users of designated
8 accounts to access, alter, and use the confidential user-information of a primary
9 account, within profile defined limits established by the owner/user of the primary
10 account. Within this profiling system, transient use accounts can be established
11 to support one-time or time-limited transaction accesses to profile defined
12 confidential user-information.

13 Another advantage of the present invention is that a requested set of
14 confidential user-information can be provided to a partner site with little or no
15 interaction with the user. A user-interface control, invoked by a single-click user
16 action or autonomously activated by the loading of a Web page, initiates the
17 information request, with pre-qualified confidential user-information then being
18 returned to the partner site. The pre-qualification of confidential user-information
19 is constrained by the profile and partner site typing functions of the present
20 invention. Thus, the pre-qualification of confidential user-information may flexibly
21 release specific confidential user-information automatically or require the user to
22 confirm release of specific confidential user-information received.

23 A further advantage of the present invention is that relatively little
24 configuration, programming, or management burden is placed on the partner
25 sites in connection with the utilization of the present invention. Integration of the

1 partner sites with the secure information server of the present invention requires,
2 in preferred embodiments, a single, simple post-processing step to process a new
3 or revised Web page. The post-processing provides a user-interface control
4 button coded with the request for the confidential user-information required to fill-
5 in the form presented by the Web page. The Web-page developer need only then
6 place the button on the Web page to complete the integration of that particular
7 page with the repository server system of the present invention.

8 Still another advantage of the present invention is that a user can securely
9 and reliably fill-in a partner site Web page form with no more than a single
10 mouse click. Once a user has at least indirectly logged onto the information
11 server, a secure, time limited session is established allowing a partner site to
12 request and transparently receive confidential user-information pre-authorized by
13 the user for release to that partner site. A single click can be used, as in the case
14 of a login, to initiate the partner site request. Alternately, a single click may be
15 used to confirm the acceptance of the form as filled-in. No click may be required
16 where the partner site is permitted to autonomously request the fill-in information
17 and where the applicable partner-site profile established by the user does not
18 specify a use-acknowledgment click.

19 Yet another advantage of the present invention is that the information
20 requests and transfers are routed through the user's computer. Encryption of the
21 information released, as well as all information provided or edited by the user, is
22 therefore enforced by the information server. For transactions between a user and
23 partner site requiring or just desiring user-identity validation, the establishment of
24 the information server account and subsequent authenticating email, postal,
25 encrypted key-card contacts allows authentication of the client-user to the

1 information server. This information may be securely passed directly to the
2 partner site to authenticate a user. Alternately, the information server may provide
3 its own authentication credentials to the partner site as a proxy for the client-user,
4 where present and prior interactions between the information server and client-
5 user are of a sufficient nature to warrant proxy validation.

6 A still further advantage of the present invention is that all accesses to the
7 information stored in a user account and all requests for and releases of data can
8 be logged and reported to the user by email, post, or through the account directly.
9 Additionally, information provided from a partner as a receipt in connection with
10 some transaction can be captured and stored for the user in the user account.
11 Capture of this information informs the user of the nature of the transaction and,
12 also, the particular profile used and data released in connection with the
13 transaction. The transaction confirmations and the collection of transaction
14 receipts both serve as checks against unadvised and fraudulent use of the
15 confidential user-information.

16 Still another advantage of the present invention is that it provides a number
17 of security capabilities, some pro-active and others based on usage reports
18 provided to the user. A proactive security measure includes the prevention of
19 identical credit card information being entered in two or more unrelated user
20 accounts existing on the information server. A reporting measure is that all
21 transactions are logged and are available to being viewed. Since the information
22 requests are routed through the user's computer, the IP address and other
23 identifying information may be logged along with the information provided by the
24 partner site. Also, the partner site is preferably required to establish an account
25 with the information server. Thus, the information server may enforce a positive

1 identification of the partner site, optionally including a reverse-DNS match, before
2 any information is released.

3
4 Brief Description of the Drawings

5 These and other advantages and features of the present invention will
6 become better understood upon consideration of the following detailed
7 description of the invention when considered in connection with the accompanying
8 drawings, in which like reference numerals designate like parts throughout the
9 figures thereof, and wherein:

10 Figure 1 is a block diagram of the network communications system
11 environment that the present invention is preferably directed;

12 Figure 2A is a process flow diagram of a preferred method of operation
13 between a partner site, user, and information server system in accordance with a
14 preferred embodiment of the present invention;

15 Figure 2B is a representative view of an exemplary partner site form and
16 active button for initiating an information request connection, on behalf of a
17 partner site to an information server system in accordance with a preferred
18 embodiment of the present invention;

19 Figure 3 is a block diagram of the processes and procedures implemented
20 by an information server system in a preferred embodiment of the present
21 invention;

22 Figure 4 is a process flow diagram of the partner site system request for
23 and receipt of information from an information server system in accordance with
24 a preferred embodiment of the present invention;

1 Figure 5 is a process flow diagram of an information server system
2 handling and responding to information requests from a partner site;

3 Figure 6 is a process flow diagram detail of the parsing of an information
4 or other request received by an information server system in accordance with a
5 preferred embodiment of the present invention;

6 Figure 7 is a process flow diagram showing the preferred post-processing
7 integration of an information server system with a partner-site Web page form;
8 and

9 Figure 8 is a process flow diagram showing the preferred pre-processing
10 integration of an information server system with a partner-site receipts posting
11 Web page.

12 13 Detailed Description of the Invention

14 As generally illustrated in Figure 1, the environment preferably addressed
15 by the present invention includes a typically public-use communications network
16 12, such as the Internet, that permits a user of a client system 14 to conduct
17 information transactions over the network 12 with any of the partner site servers
18 16, 18, 20 and an information server system 22. The partner site servers 16, 18,
19 20 represent any network accessible computer systems that provide or require a
20 login identification by the user, that request form-entry type information, or that
21 may submit information, such as receipts, on behalf of a user to the information
22 server system 22. The partner site servers 16, 18, 20 may be electronic
23 commerce sites, where the user is allowed to order or purchase goods or services.
24 Site-specific Web page forms are presented to the user to obtain identifying
25 information, such as a login name and password, and other transaction-specific

1 information prior to completing a user transaction. Electronic receipts and
2 receipt-type data, generated in connection with an ecommerce transaction or
3 independently generated and supplied, such as in the case of warranty and
4 product registration, and purchase incentive coupons, are preferably received
5 from partner sites.

6 In accordance with the present invention, the partner site servers 16, 18,
7 20, present an additional user-interface (UI) control, such as a clickable button,
8 on Web pages to allow a user to initiate the retrieval of confidential user-
9 information desired to complete a specific data-entry form. The UI control may
10 also be used to initiate or cause the submission of receipts or receipt-type data for
11 storage with the information server system for the benefit of the user. Other
12 controls, such as check-boxes, selection lists, and radio buttons, as well as pre-set
13 site and user-specific site configuration options, can be used as alternative
14 interface controls.

15 In the case of a Web page form, the user activation of a user-interface
16 control, either directly as through a button click or indirectly through the triggering
17 of a pre-set, a request is issued, preferably using an HTTP Get command or
18 alternately a Post command, on behalf of the corresponding partner site server
19 16, 18, 20 destined for an information server system 22 that includes a processor
20 system 24 that manages and controls access to an information repository 26.
21 When received, the request contains or is accompanied by sufficient information
22 to authenticate the partner site server 16, 18, 20 and the client system 14 to the
23 information server system 22. The request also identifies the information needed
24 to complete the partner site form presented to the user. This identification of the
25 information requested can be an explicit coded listing of the requested

1 information. Alternately, the identifier is an indirect reference, which is
2 processable by the information server system 22, to obtain a corresponding list
3 of the requested information. Preferably, the identifier is constructed as a hybrid,
4 containing explicit data field references for handling dynamic data requirements
5 and a storage reference for data field references that are well anticipated or static.
6 Using the hybrid specification of data references allows the dynamic or run-time
7 complementing and overriding of the static set of data field references.

8 In each of these cases, each form field is named such that when this
9 requested information is returned to the partner site, each datum returned is
10 named with a corresponding field name which is the partner site form field
11 assigned name, functionally allowing the form to be autonomously filled-in.
12 Consequently, a single button click, which may be implicitly provided where a pre-
13 set is used, is all that is required to complete a form presented by a partner site.

14 To operate within the preferred embodiments of the present invention, the
15 user is required to initially establish a user-account on the information server
16 system 22. In establishing this account, the user is allowed to select or is assigned
17 a unique user-identifier, such as a username and password. This identifier,
18 potentially further based on an encrypted key token, is used to subsequently
19 identify the user to a partner server system 16, 18, 20 that has established a
20 partner-account with the information server system 22.

21 As part of creating or later updating the user account, the user is enabled
22 to provide and store confidential user-information, broadly defined as any
23 information that is reasonably personal to the user, such as name, age, shipping,
24 billing, and home addresses, multiple credit card information, social security
25 number, telephone numbers, medical record numbers, personal interests lists,

1 wish lists, receipts, registrations, survey answers, other use data and files, and
2 various user-oriented and partner site-oriented preferences. Preferably, the user
3 is permitted to establish different named profiles and aliases for information
4 subsets stored in the user account. In general, the profiles define particular user-
5 controlled views to the confidential user-information stored in the user-account.
6 For example, different sets of credit card information, shipping addresses, and
7 other relevant information may be directly named or aliased to descriptive names,
8 provided by and easily identified by the user, used to describe general uses, such
9 as business, medical, and personal or particular uses, such as a specific corporate
10 travel account. These named profiles can then be identified or associated for use
11 with other profiles used, for example, to identify specific partner sites and include
12 other confidential user-information, allowing the user to define site-specific and
13 role-based constraints on the information that may be modified or released.
14 Named profiles, such as "login only," "company purchase plan," and "games,"
15 may be established for use in constructing other site-specific profiles. Preferences
16 may be stored globally by the information server system 22 for controlling,
17 constraining, and defining the interoperation of the information server system 22
18 individually with partner site servers 16, 18, 20 and with the user. Overriding
19 preferences may be established in individual profiles for closely controlling,
20 constraining, and defining the interoperation of the information server system 22
21 with specific partner site servers 16, 18, 20 and the user.

22 Profiles that establish roles for partner sites that do not then have partner
23 site accounts established may, in preferred implementations, provide for the
24 creation of such accounts. Thus, for example, a restricted access profile created
25 to allow a doctor or laboratory to transfer in and review profile defined medical

1 data also creates an account for the doctor or laboratory if one is not pre-existing.
2 Time-limited accounts established to provide payment to incidental vendors of
3 goods can also be supported by a user's creation of a corresponding time and
4 value limited user profile. Similarly, a profile providing a limited credit-line usage
5 of a parent's credit card, potentially further limited in terms of allowed product-
6 type purchases that can be made, enables the user of the identified child account
7 to access and use the data within the parent account subject to the profile
8 limitations.

9 Preferably then, each partner site server 16, 18, 20 is also required to
10 establish a partner-account, which is specific to one or more sites, on the
11 information server system 22. The partner-accounts are each assigned a unique
12 identifier, which must be provided with any partner-site information request. The
13 information server system 22 also requires coordinated receipt of the user-
14 identifier. In accordance with the present invention, the user-identifier is
15 independently provided from a client system stored cookie directly to the
16 information server system 22. The user-identifier is not provided to the partner-
17 site. The required independent receipt of both the partner and user-identifiers,
18 which are only commonly known to the information server system 22 provide a
19 significant level of authentication of the partner site servers 16, 18, 20, as well
20 as the client system. The partner-accounts may also store data defining additional
21 authentication protocols that can be used to ensure that server impersonation is
22 precluded. Another use of the partner-accounts is to provide storage for mapping
23 tables for converting between well-known data codings, as used by the
24 information server system 22, and any alternate coding set used by a particular
25 partner site. Other information, such as the identification of a different URL to be

1 used for returning user information or particular requirements of a particular
2 partner site server, can also be stored in individual partner accounts.

3 A preferred transactional implementation of the process of the present
4 invention is shown in Figures 2A and 2B. The process flow 30 preferably starts
5 with user actions 32, typically Web navigational transactions with some partner
6 site server 16, that results in the user being presented with a form 52 to be
7 completed 54, 56. This form includes the user-interface control 58, hereinafter
8 referred to as the OneID™ button, which is coded with an HTTP Get command for
9 issuance to the URL of the information server system 22, all provided in
10 accordance with the present invention. The HTTP Get command also preferably
11 includes the partner-identifier and one or more identifiers that identify or represent
12 the confidential user-information requested by the partner site server 16. Since
13 the information server system 22 is known to the partner site server 16, the target
14 URL of the information server system 22 can be pre-emptively specified with
15 respect to a particular Get command. Conversely, the partner site URL is either
16 also coded into the Get command or available by lookup by the information
17 server system 22.

18 When the user selects the user-interface control 58, the HTTP Get
19 command is finally prepared and issued by the client computer system 14, in
20 effect, on behalf of the partner site server 16. This final preparation include
21 incorporation of client system specific data, such as transaction specific identifiers
22 and values, to be included in the Get command. The issuance of the Get
23 command by the client system 14, as opposed to the partner site server, allows
24 information from the client system 14 to be included independent and unseen by
25 the partner site server 16. The issuance of the Get command allows cookies and

1 potentially other data from the client computer system 14 to be passed on to the
2 information server system 22 as part of or associated with the Get command.

3 The issuance of the HTTP Get command and included information is
4 preferably performed using a secure protocol, such as provided by secure
5 transactions layer, such as the Secure Sockets Layer (SSL). Use of the secure
6 protocol is preferably maintained as between the partner-site server 16, client
7 system 14, and information server system 22 until a response to the issued request
8 is eventually returned to the partner-site server 16. Preferably, the information
9 server system 22 requires secure transactions between the client system 14 and
10 the information server system 22 whenever confidential user-information is being
11 manipulated.

12 The client system 14 participates substantively in each communication
13 transaction involving the information server system 22 and any of the partner site
14 servers 16, 18, 20. With each data transaction, the client system 14 provides any
15 applicable cookies stored by the client system to the information server system 22.
16 Preferably, this cookie data includes an identification of the client system 14 and
17 a time signature representing the user of the client system 14 is logged in on the
18 information server system 22. The cookie containing the time signature is
19 preferably stored on the client system 14 as a transient cookie with a short time-
20 to-expiration limit as set by the information server system 22. Each
21 communication between the client system 14 and the information server system
22 22 may replace or update any or all applicable cookies stored by the client system
23 14.

24 Issuance of the HTTP Get command to the information server system 22
25 gives effect to a top level or overarching transaction between the information

1 server system 22 and a partner site system 16. In response to the receipt of this
2 Get command, the information server system 22 may execute any number of
3 intervening HTTP or other transactions with the client system 36 or simply return
4 the requested data in a Get response to the client system 14 with the partner site
5 system 16 as the effective target. The client transactions preferably include, but
6 are not limited to the set of transactions set forth in Table I.

7 Table I
8 Client/Information Server System Transactions

9 Login:

10 the client time signature cookie has expired or has been removed; a login
11 screen for the information server system 22 is presented to the user of the
12 client system 14.

13 Profile Choice and Confirmation:

14 no profile has been assigned to this partner server 16 or if assigned, has not
15 been enabled for autonomous response to the request; a profile choice or
16 confirmation screen is presented to the user of the client system 14.

17 Profile and Information Server System Data Update:

18 the form data requested by the partner server system 16 is not in the
19 selected profile or is not stored by the information server system 22; the user
20 is presented with screens to select a different profile, enable the requested
21 information to be visible in a selected profile, use the existing available data
22 in responding to the partner server system 16, or to enter the data into the
23 information server system 22; data that is required by the partner server
24 system 16 is distinguished from optional data identified in the request.

Table I
Client/Information Server System Transactions

Create and Edit Profiles:

the user may create new profiles and revise existing profiles to contain specific sets of information; new information may also be provided for storage by the information server system 22 and, thus, made available for inclusion in any of the profiles; any profile may be marked for autonomous use in response to a request from a particular partner site server 16, marked to require confirmation before responding to a data request by any particular partner site server 18 or marked to offer the creation or selection of a profile corresponding the requested data where no profile has prior assigned to a particular partner site server 20.

Messages and Warnings:

a message or warning is presented to the user where invalid or unknown data is requested by any partner site server, where the partner site server account has been closed or terminated, or where the partner site server or client system login cannot be authenticated.

A response to the form data request by the partner site server 16 is potentially supplemented and approved 36 by the user of the client system 14 through actions taken in intervening HTTP transactions with the information server system 22. Where the user is not already logged in to the information server system 22, an applicable profile requires the confirmation of the release of some confidential user-information, or the responsive information is either not available within the applicable profile or user-account altogether, suitable Web page forms are preferably generated and presented to the user for completion. This new confidential user-information is then stored by the information server system 22 and made available through whatever profiles are designated by the user. Conversely, where the user is logged-in to the information server system 22 and

1 the requested confidential user-information is cleared for automatic release to at
2 least the requesting partner-site, no overt confirming user action 36 is required.

3 Once the release of confidential user-information is approved, whether
4 directly or indirectly, the applicable profile-delimited responsive data is returned
5 as a response to the initial Get command issued by the client system 14 on behalf
6 of the partner site server 16. The client system response 38 in turn provides form
7 data to the partner site server 16, along with any applicable partner-site cookies.
8 As part of the Get command response processing, the named fields of the form
9 are filled-in. If all of the requested field data identified by the partner site server
10 16 as required is received, the partner site server 16 may simply proceed and
11 process the form using the provided data. This is preferably the action taken
12 when the form represents a login request for the partner site server 16.

13 Alternately, the partner site server 16 may autonomously utilize the form
14 with the provided data and await further user actions 40, such as the entry of
15 additional form data or an explicit submission request from the client system 14.
16 Such further form data may be information for required form data fields not
17 provided by the information server system 22 or possibly to encourage the user
18 to complete optional data fields not filled in with data from the information server
19 system 22. In either case, a submission button or the like is conventionally
20 provided by the partner site server 16 on the form page to enable the user to
21 signal that the form has been completed to the extent desired by the user.

22 The information server system 22 and particularly the server processor 24
23 is detailed in Figure 3. The processor 24 preferably includes a network interface
24 60 that connects with the network 12. A security module 62, preferably
25 implementing the SSL protocol and included as a software component within a

HTML, WAP, XML or other Web server 64, operates as an interface to the network interface 60. Information, such as the component parts of the form data received in response to an HTTP Get command, are provided through the Web server 64 to a process manager 66. This process manager 66 may be implemented as a server-side application. In any particular implementation, the process manager 66 preferably operates to stage the series of events needed to respond to whatever Web request that is presented to the network interface 60. Some of these steps may entail the preparation and presentation of information on a virtual or remote interactive user-interface 68 to a user of the client system 14 to, for example, permit additional information to be entered into the corresponding user record as stored in the data repository 26 or present messages and warnings to the client system 14 and potentially to the partner site server 16.

Any data from the user and partner account records, is provided individually or collectively 70 from some number of supporting processes 72_{1-N}. This information may be requested by and returned to the process manager 66 and the virtual interactive user-interface 68. These processes 72_{1-N} variously support the client system 14 and partner site server 16 requests and may include, but are not limited, to the processes identified in Table II.

Table II
Information Server System Processes

Authentication Process:

supports the verification that specified client and partner accounts are active and that any provided IDs, passwords, certificates or tokens are valid.

Profile Process:

supports the selection of profiles as well as the creation and editing of profile preferences and contents.

Table II
Information Server System Processes

Form Fill-in Process:

supports the identification and selection of data corresponding to the codes provided with a form data request, including resolving code to available data ambiguities, from an identified profile.

Transaction Process:

supports the suspension of a current form data request while potentially multiple user transactions are executed in support of other processes.

Receipts and Receipts-type Data Reporting Process:

supports the collection, updating, and reporting of user receipts, coupons, registration acknowledgments, and other receipt-type data.

Transaction History Process:

supports the identification and reporting of user and partner detailed purchase transaction form fill-in and other activity history records.

Data Update Process:

support information server system requests presented a user to obtain particular data, such as may be needed to suffice a form data request, and to record the details of individual purchase transactions for both the partner and client users.

As generally shown, the information provided by the supporting processes 72_{1-N} is returned to the process manager 66 or the virtual interactive user-interface 68, based on the identified source of the information request. The process manager 66 may process this information to determine whether any further steps are necessary before returning data to the client system 14. For example, the form fill-in process 72₃ may indicate either that an assigned profile does not

1 include all or, at least, the required data requested or that the user record simply
2 does not contain some part of the data requested. Thus, depending on the
3 particular response of the form fill-in processor, the process manager 66 may
4 choose to invoke other processes 72_{1-N} , such as the transaction process 72_4 , the
5 profile process 72_2 , and the data update process 72_N .

6 The data needed to support transactions with the user are prepared by the
7 virtual interactive user-interface 68 and forwarded on to the client system 14
8 through the HTML server 64. Similarly, the data responsive ultimately to a partner
9 site server 16 request is prepared and returned through the HTML server 64.

10 The support processes 72_{1-N} may, as appropriate, communicate data to
11 and from the data repository 26. These communications are preferably supported
12 through a software interface 74 to an object or relational database management
13 system that, in turn, manages the reading and writing of account records stored
14 by the data repository 26. Using an object database management system may
15 be preferred.

16 Referring now to Figure 4, a preferred partner site server 16 process is
17 presented. The partner site server 16, in response to web navigation commands
18 presents 82 a form, such as form 52, to the user of a client system 14. The user
19 may simply choose to complete the form directly and continue 84 with the partner
20 site server 16 controlled process. Alternately, the user may choose to invoke a
21 repository access process by clicking 86 the provided button 58. In response, the
22 client system 14 issues 88 the button embedded predefined coded request for the
23 information needed to complete the form. Preferably, required information is
24 distinguished from optionally entered information in the coded request. This
25 coded request preferably contains a URL containing a Get command and

1 identifications of the source partner site server 16 and target information server
2 system 22. The Get command also preferably contains a reference to a mapping
3 of the named form fields for which information is requested and the
4 corresponding data fields supported by the information server system 22.
5 Preferably, the mapping is predefined and stored by, in part, the information
6 server system 22.

7 A response to the coded request is preferably received 90 and parsed 92
8 to recover the coded information returned. This information is then used to fill-in
9 94 the form presented by the partner site server 16. Additional codings or other
10 information may also be returned to the partner site server 16 to specify whether
11 the filled-in form should be redisplayed to the user and await further user input
12 or be automatically submitted to the partner site server 16 for continued 84
13 processing.

14 Where the network transmission of the response is incomplete or invalid,
15 a failure report may be issued 96 to the user and, preferably, to the partner site
16 server 16. The user notification at least allows the user to be aware of the failure.
17 The notification to the partner site server 16 preferably enables continued
18 processing 84 through an error management routine that may simply reissue the
19 coded request to the information server system 22 or present the user with the
20 choice to abort or reinitiate the process of requesting information from the
21 information server system 22.

22 A partner site server 16 can provide receipt-type data to the information
23 server system 22. While this data may be submitted autonomously by the partner
24 site server 16, preferably a Web page containing the information to be submitted,
25 in effect a pseudo-form page, is presented to the user. Either in response to a

1 button click 86 initiating the submission of the data or a page display trigger, the
2 data is prepared 102 by associating each component of the data with an explicit
3 data field name supported by the information server system 22, or a pseudo-field
4 name that is then mapped to a corresponding data field name. Where the
5 receipt-type data is dynamically generated by the partner site server, the content
6 of the Get command, or alternately a Post command, must be dynamically
7 prepared 100. A URL including the Get command data then built 102 and sent
8 88. The response received 94 is preferably a confirmation acknowledgment
9 message 98, indicating that the data has been received and appropriately
10 handled by the information server system 22. After receiving an acknowledgment,
11 the partner site server 16 continues 84 typically to interact with the user of the
12 client system 14. Where a negative acknowledgment or some other failure
13 message is received, the failure is reported 96 preferably to the partner site server
14 16, which can the continue 84 and handle the error condition.

15 The preferred information server system 22 process is shown in Figure 5.
16 Inbound requests from a client system 14 are received 112 as information server
17 requests. This request is automatically coupled with a client time-signature cookie,
18 if available. If the signature cookie is not present or has expired, the user is
19 permitted to logon 114. Provided there is a successful login, the data from an
20 expired time signature cookie is then effectively replaced by the new login
21 information.

22 The request is then examined to retrieve the account information, including
23 the partner-identifier, of the partner site server 16. The client-identifier is
24 obtained from the client cookie or newly logged in account. In performing an
25 account lookup 116, if either account is not found or is not active, a failure

1 message 118 is returned by the information server system 22. Where both site
2 accounts are found and are active, a site coded request function is identified 120
3 from the request. Typically, the site function identifies a specific request for data
4 to fill-in a form. The profiles defined in the user-account, as stored by the data
5 repository 26, are then examined to identify 122 a profile associated specifically
6 or by general criteria with the identified partner site server 16. If such a profile is
7 not found, the user may be prompted to enable setup of a new site 124,
8 producing update data reflecting a change in the associated user account, which
9 is then updated 126 to the data repository 26. Where a new site is setup or where
10 no profile is associated with a prior setup of the site, or where the site-identified
11 profile is set to require a re-selection of the applicable profile, the user is
12 presented with a form-based opportunity to select and apply an existing profile
13 from the user account. Where a profile is selected, the user account is
14 correspondingly updated 126. The user is then permitted to immediately use the
15 selected profile or setup 130 and select a new profile for the identified site. In
16 both instances, the user is preferably also permitted to edit 130 the selected
17 profile.

18 The selected profile is then qualified, particularly as to whether sufficient
19 information is present in or through the profile to fully respond to the outstanding
20 information request. A new data query, if needed, is presented 134 to the user
21 to enable profile access to data stored at large in the user account and to obtain
22 information identified in the information request but not present in the user
23 account. In the former case, the selected profile is updated 126 to indicate that
24 additional information is at least logically included in the selected profile. In the
25 later case, the new information entered is updated 126 to the user account and

1 again the selected profile is updated 126 to indicate that additional information
2 is at least logically included in the selected profile.

3 The selected profile is also qualified 132 as to whether use of the profile
4 is pre-approved for automatic response or requires user approval prior to a
5 response being issued back to the partner site server 16. Where use of the profile
6 is pre-approved, the request responsive data is collected from the selected profile,
7 coded into Get response and issued 136 to the client system 14 for further return
8 to the partner site server 16. Where user approval 138 is required, the user is
9 presented with a confirmation form, preferably including an identification of the
10 current information to be submitted to the partner site server 16. The user may
11 then approve issuance 136 of the response, select another profile 128, create a
12 new profile 130, and edit 130 the selected profile.

13 Another partner site function is the submission, by a partner site server 16,
14 of receipt-type data, which may include data describing a single purchase
15 transaction, a historical set of transactions, and other activity data for storage in
16 the user account. Such activity data is recovered 140 from the partner site server
17 16 request. The data is updated 126 to the data repository 26. An
18 acknowledgment of the successful updating of the user account data may
19 optionally be returned to the partner site server 16. In similar fashion, other
20 function identified actions 142 may be recognized 120 and suitable responses
21 prepared. These responses may be presented as acknowledgments 144 or coded
22 responses 136 containing data obtained from the data repository 26.

23 Figure 6 shows a preferred process flow 150 for user interactions directly
24 with the information server system 22 from the client system 14. User interactions
25 are preferably supported through a public Web site (not shown) and, in general,

1 presented as one or more Web pages containing the selections available to the
2 user and fields that enable user entry and editing of the data stored in an account
3 record. This Web site is preferably hosted by or on behalf of the information
4 server system 22. The Web site may thus be considered part of the information
5 server system 22.

6 When a selection or entry is submitted by the user, the resulting URL
7 packaged request is submitted, received and examined 112. If the accompanying
8 time signature cookie is present and not expired, the request embedded within the
9 received URL is further examined to recover the identified function 120 selected
10 by the user. Alternately, where the time signature cookie has expired, the
11 information server system 22 presents the user with a login screen 114 prior to
12 further examination of the received request.

13 Any number of different function requests can be submitted to the
14 information server system 22. Choice of a specific function may be by a user
15 through a subsequent, more detailed selection list presented as a secure Web
16 page form to the user. As represented in Figure 6, a report of partner transaction
17 data and other historical information may be requested. A report is prepared 154
18 and returned 156 to the user preferably as another Web page. Similarly, a
19 function requesting a status check 158 of pending purchases results ultimately in
20 the preparation 160 of a corresponding status report and return 156 of the status
21 report as a Web page. Receipt-type data can also be reviewed 162 and reported
22 164 to the user.

23 The information system server 22 preferably responds to a function request
24 ultimately specifying the modification of some account record data by presenting
25 a corresponding Web page to permit entry of the modifications. Such

1 modification may include the editing 166 of profiles, the informational contents
2 of the account data, the specific and general association of profiles with partner
3 sites, and various user account and profile preferences. The modified data, when
4 submitted back 168 to the information server system 22, is stored in the user
5 account. An acknowledgment of the secure receipt and storage of the data may
6 then be returned 156 by the information server system 22. Alternately, a
7 confirmation Web page may be presented to allow the user to verify the data
8 before being committed to the user account within the data repository 26.

9 Other operations on the user account can be similarly provided by pre-
10 establishing an identifiable 120 request-type. Execution of the corresponding
11 function can then be performed by the information server system to return 156 an
12 appropriate response to the user.

13 The preferred process 176 of integrating the information server system 22,
14 in accordance with the present invention, with the Web page forms of a partner
15 site 16 is shown in Figure 7. In order to ease and place a minimum burden on
16 the development and maintenance of partner site Web page forms, the preferred
17 process is implemented as a post-processing step relative to the design and
18 development 178 of a Web page form. The post-processing step begins with the
19 submission of the Web page form to a software mapping tool hosted, directly or
20 indirectly by the information server system 22. In order to submit the Web page
21 form, the developer utilizes an interactive process 180 to receive a login form.
22 The developer is preferably required to login to the partner site account and
23 request the submission of the Web page form 182. The submission process is
24 carried out by uploading the Web page form code through a form provided by
25 the information server system 22. The upload may be specified by the developer

1 providing a URL to the form page and initiated by a button click leading to an
2 activity data transfer of the Web page code directly to the information server
3 system 22. Alternate manners of submitting a Web page form, such as through
4 pasting, can be supported.

5 When received, the Web page form code is passed to a backend process
6 184 to be parsed 186. This parsing operates to identify the names of the form
7 fields embedded in the Web page form. Based on the names parsed from the
8 form, a mapping display process is then executed to define, to a reasonable
9 extent, a likely mapping of the form field names to the names of the data fields
10 defined for the data repository 26. The resulting mapping table is then passed to
11 the interactive process 180 for display 190 to the Web page developer. The
12 displayed form allows the developer to correct and complete the association of
13 form field names to data field names. While a form field name such as "First
14 Name" could be autonomously mapped to a likely corresponding data field
15 named "\$o_firstname\$," a form field name "PrimaryN" is unlikely to be correctly
16 mapped to "\$o_firstname\$." The mapping form preferably allows form field
17 names to be associated with data field names using a simple clickable interface.

18 Another mapping issue handled by the mapping tool of the present
19 invention involves specifying value format conversions. Preferably, the mapping
20 form allows a Web page form developer to construct value format conversions
21 using parsing, logical combination, concatenation, translation, and other
22 functions and operators. Conversions defined using these functions and
23 operators are applied against identified data fields of the data repository to create
24 a value format conversion appropriate for returning data from the information

1 server system 22 in a manner that matches the desired value format of a Web
2 page form field.

3 For example, where a single form field requires a full name, a format
4 conversion is required where the data repository separately carries first, middle,
5 and last names. For a form field name of "p_name" and data field names
6 "\$o_firstname\$," "\$o_middlename\$," "\$o_lastname\$," a value format
7 conversion can be constructed using concatenation as:

8 p_name=\$o_firstname\$+\$o_middlename\$+\$o_lastname\$.

9
10 Format conversions are also required where, for example, a date must be
11 provided in a locale specific format or credit card numbers must be provided with
12 particular punctuation or broken-up into four component number fields for entry.
13 To provide punctuation, specifically using a colon in this example, a value format
14 conversion for a form field named p_creditcard number can be constructed using
15 parsing and concatenation:

16 \$oa_1\$=\$subst(o_ccnumber, 1,4)\$;

17 \$oa_2\$=\$subst(o_ccnumber, 5,8)\$;

18 \$oa_3\$=\$subst(o_ccnumber, 9,12)\$;

19 \$oa_4\$=\$subst(o_ccnumber, 13, 16)\$;

20 p_creditcardnum=\$oa_1\$%3A\$oa_2\$%3A\$oa_3\$%3A\$oa_4\$;

21
22 where %3A is the encoded format of ":".

23 Other instances and types of format conversions can be numerous. Since
24 the value format conversion is performed by the information server system 22, a

1 flexible and, as needed, large library of conversion functions and operators may
2 be maintained universally for use by Web page developers.

3 Predefined, or aliased, conversions are preferably also supported by the
4 mapping tool. In the preferred embodiments of the present invention a date data
5 field is aliased to a number of locale specific date data fields. Referencing the
6 data field name of an aliased date data field is recognized by the information
7 server system 22 as requiring a corresponding conversion. Thus for a form field
8 name "p_date," a mapping of "p_date=\$o_dateEPlocale\$" is logically expanded
9 and executed as:

10 `p_date=$european_date(o_date)$;`

11 where the pre-defined function "european_date" provides the appropriate
12 conversion. Thus, many common conversions may be easily represented as
13 merely alternative data repository data field names. Such pre-supplied conversion
14 function aliases, combined with the potential of allowing a developer to store
15 custom conversion functions in the partner site account, greatly eases the process
16 of defining the form field name mapping.

17 In connection with performing field name mapping, the present invention
18 permits the Web page form developer to define and name custom or "dynamic"
19 data fields 196 and then map form field names to those data fields. This allows
20 the Web page developer to expand the base of information carried by the
21 information server system 22 on behalf of the partner site server 16. When a user
22 encounters a Web page form that includes a dynamic data field, the information
23 server system 22 will present the field to the user for completion in the same
24 manner that predefined data repository 26 fields are presented to request data
25 entry or prompted for inclusion in the current applicable profile. Where data is

provided to the information server system 22 for a custom data field, the data object representing the profile is preferably extended to provide storage for the entered data. Subsequently, references from the partner site server 16 to the dynamic data field name will return the corresponding stored data. As the creation and subsequent management of the dynamically created data fields is handled for the partner site server 16, the only significant requirement placed on the Web page developer is to associate their assigned data field name with a consistent definition or understanding of what the stored data represents. Since this definition is specific to the partner site account, the developer is well capable of maintaining such a definition.

Once the mapping 190 of a Web page form is completed, the developer submits the mapping 198 for generation 200 of a map coding block. Preferably, this map coding block includes a structured set of mapping statements, such as those illustrated above. In a preferred embodiment of the present invention, a generated map coding block will be of the general form:

```
http://www.oneid.com/site/partner.jsp? // target URL
method=post                          // transport method
&sid=230776                          // partner-identifier
&action=form_encode(formpage_URL)    // source URL
&p_map=form_encode( \
    p_date=$o_dateEPlocale$& \
    p_name=$o_firstname$+$o_middlename$+$o_lastname$& \
    $oa_1$=$subst(o_ccnumber, 1,4)$& \
    $oa_2$=$subst(o_ccnumber, 5,8)$& \
    $oa_3$=$subst(o_ccnumber, 9,12)$& \
    $oa_4$=$subst(o_ccnumber, 13, 16)$& \
    p_creditcardnum=$oa_1$%3A$oa_2$%3A$oa_3$%3A$oa_4$&\
    p_fieldname1=lib_conversionX($o_datafieldnameA$)
)
```

1
2 The generated map coding block is then wrapped 202 preferably with the
3 HTML coding for a simple UI button 58. The resulting UI code, including the map
4 coding block is then presented to the developer for download 204. In connection
5 with the preferred embodiments of the present invention, the developer will then
6 need only to insert 206 the downloaded UI code in the previously prepared form
7 Web page in a manner that visually places the UI button 58 at an appropriate
8 location on the Web page form. The Web page form is then ready to publish 208
9 using any conventional Web page deployment tool.

10 An alternate process 210 of using the software mapping tool is shown in
11 Figure 8. The process 210 may be used where the Web page developer wishes
12 to use the mapping tool before preparation of a Web page form 178. The
13 process 210 is perhaps more typically used where the developer is preparing a
14 receipts-type data display Web page and wishes to submit the data to the
15 information server system 22. In either case, the mapping tool is used as a pre-
16 processing-type step to generate UI code that can be included on a Web page.

17 Similar to the process 176, the developer initiates 212 the mapping
18 process 210 by logging in and setting 214 the tool to a pre-processing mode. A
19 comprehensive mapping table is prepared. The mapping display 190 is then
20 presented to the developer. While place-holder field names may be defined and
21 used to map against the data repository data fields, the developer may choose to
22 directly use the data repository data field names. These place-holder field names
23 are used as pseudo-filed names, since a dynamically generated receipts-type Web
24 page will not include any form fields. These pseudo-field names are therefore
25 assigned by the developer to different data elements presented on the receipts-

1 type Web page as part of the mapping 192. The pseudo-field names may be of
2 particular use where the presented data must be converted to a value format
3 defined by a data repository data field, generally as described above. Alternately,
4 use of data repository data field alias names may be sufficient to implicitly convert
5 the developer chosen format of the receipts-type data to a value format
6 appropriate for storage in the data repository 26.

7 Mapping 192, value format data conversion 196, as well as the creation
8 of dynamic fields for storing unique receipts related data, such as a shirt pattern
9 type, size, or other information descriptive of the receipted transaction, are all
10 available to the developer through the mapping display 190. Once the mapping
11 190 is complete, the mapping is submitted 198, a map coding block generated
12 200, and preferably wrapped with the HTML coding for a simple UI button 58.
13 The resulting UI code is then presented for downloading 216 to the developer.
14 Once retrieved, the UI code can then be used in the preparation of the Web page
15 form or receipts-type data page 218 by the developer. When completed, the Web
16 page can then be published using a conventional deployment tool.

17 Thus, a user identification system, including the capability maintain and
18 securely supply user data to third-party sites, has been described. While the
19 present invention has been described particularly with reference to HTML and
20 Web page based transactions, the present invention is equally applicable to e-
21 commerce sites utilizing other and additional communications and data sharing
22 protocols, including eHTML, XML, SGML, and wireless systems. The present
23 invention is also applicable to any site that presents a form for user data fill-in.

24 In view of the above description of the preferred embodiments of the
25 present invention, many modifications and variations of the disclosed

embodiments will be readily appreciated by those of skill in the art. It is therefore to be understood that, within the scope of the appended claims, the invention may be practiced otherwise than as specifically described above.